Non-deterministic noiseless amplification via non-symplectic phase space transformations

Nathan Walk,[1] Austin P. Lund,[1] and Timothy C. Ralph[1]

[1]*Centre for Quantum Computation and Communication Technology*
*School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia**

We analyse the action of an ideal noiseless linear amplifier operator, $g^{\hat{a}^\dagger\hat{a}}$, using the Wigner function phase space representation. In this setting we are able to clarify the gain g for which a physical output is produced when this operator is acted upon inputs other than coherent states. We derive compact closed form expressions for the action of N local amplifiers, with potentially different gains, on arbitrary N-mode Gaussian states and provide several examples of the utility of this formalism for determining important quantities including amplification and the strength and purity of the distilled entanglement, and for optimising the use of the amplification in quantum information protocols.

I. INTRODUCTION

Optical quantum communication has resulted in numerous protocols that achieve classically impossible tasks including teleportation [1, 2], quantum key distribution [3, 4] and super-dense coding [5, 6]. Furthermore, several of these have seen experiments ranging in sophistication from proof-of-principle demonstrations [7–11] to implementations approaching real world conditions [12–15]. One of the great challenges that stands between these schemes and the realisation of large scale quantum information networks is the necessity of preserving often fragile quantum states in the presence of losses and other decoherence. A device that allowed for amplification to combat such effects would be extremely useful, however the laws of quantum mechanics themselves conspire to enforce a noise penalty whenever such an operation is attempted [16].

An ingenious recent approach is to circumvent these limits by designing devices that achieve genuinely noiseless amplifications in a non-deterministic but heralded manner [17]. This noiseless linear amplifier (NLA) has been the subject of considerable theoretical [18–31] and experimental [32–39] work. Applications in quantum key distribution (QKD) with both continuous variable (CV) [25, 27, 28] and discrete variables (DV) [20, 23] have been considered as well as error correction [21]. In the literature one finds two kinds of analysis. In the first place one can consider the ideal amplification operation, which is to implement $g^{\hat{a}^\dagger\hat{a}}$. In the amplification regime ($g > 1$) this is an unbounded operator, however for any particular input state one can always write down a new operator of the form $\hat{\Pi}_N g^{\hat{a}^\dagger\hat{a}}$ where $\hat{\Pi}_N$ is a projector onto the subspace spanned by the first $N+1$ energy eigenstates. This operation will result in an arbitrarily good approximation of an ideal NLA as N increases at the price of a decreased, but finite, success probability. In the second kind of analysis works thus far have utilised particular linear optics implementations such as that of the original proposal [17] or those based upon photon addition and subtraction [22, 30, 31].

Here we will adopt the first approach, and focus on gaining a greater insight into the properties and applications of the operation $g^{\hat{a}^\dagger\hat{a}}$. In Section II we will derive the action of the operation on an arbitrary state via the Moyal product and show that it has the unusual property of being a Gaussian but non-symplectic map. Furthermore we address the scenarios in which, dependent upon the state to be amplified, the NLA fails to transform into a physical output in the limiting procedure described above. Some necessary concepts in Gaussian quantum information are introduced in Section III. In Section IV we apply our formalism to obtain compact analytic expressions for up to N amplifiers acting upon N-mode Gaussian states. We give specific examples for one and two mode cases and comment more rigorously on the physicality of the operation dependent upon the input state. In Section V we consider in more detail the distribution of EPR entanglement through a general Gaussian channel which is the situation most relevant to continuous variable QKD. We show that previous attempts to represent the action of the NLA and an effective channel of the same form but with different parameters are in general insufficient. In a surprising example we show that in the for large gains the NLA has the effect of transforming an attack on one half of an EPR pair into an attack upon the other half. Finally in Section VI we conclude.

II. NLA AS A NON-SYMPLECTIC OPERATION

We can define ideal linear amplification in terms of coherent states as

$$|g\alpha\rangle\langle g\alpha| = \Upsilon(|\alpha\rangle\langle\alpha|). \quad (1)$$

We can realise Υ by

$$\Upsilon(\rho) = \lim_{N\to\infty} \Upsilon_N(\rho) \quad (2)$$

*Electronic address: walk@physics.uq.edu.au where

$$\Upsilon_N(\rho) = p_N^2 g^{a^\dagger a} \Pi_N \rho \Pi_N g^{a^\dagger a} \tag{3}$$

where the constant p_N is chosen to make the operation physical and Π_N is the projection operator defined earlier. For most of this work we will ignore p_N, it is important to say a few words about it at this point. To achieve ideal linear amplification over the entire harmonic oscillator Hilbert space requires $\lim_{N\to\infty} p_N = 0$ as the $g^{a^\dagger a}$ operator has an unbounded spectrum. However, in any realistic experiment there will be some bounds within which it is assumed that the experiment is being performed. First there will be assumed some energy bound which can be thought of as a truncation of the Hilbert space. This results in accepting a non-unit fidelity with the theoretically ideal amplifier for states which have a component outside this bound. The choice of truncation is somewhat arbitrary, but will generally be determined by the energy limits of the experiment. We can think of a sequence of operations which is indexed by the largest energy eigenstate which is allowed, which we will call N. For any finite N there is a finite non-zero p_N which one can choose for Υ_N. As N grows, p_N must reduce. In the limit as N approaches infinity, we recover the ideal operation and p_N tends to zero. The prediction we make by ignoring p_N in the theory is the state resulting from this limiting case. However we emphasise that the existing experiments have already shown that for low energy input states approaching the limiting case of ideal operation is achievable without prohibitively low success probability.

The $g^{a^\dagger a}$ operator in Wigner space is

$$\begin{aligned} G_w(x,p) &= \frac{1}{2\pi}\int e^{ipy}\langle x-y| g^{\hat{a}^\dagger \hat{a}} |x+y\rangle \quad dy \\ &= \exp\left\{\left(\frac{g-1}{g+1}\right)(x^2+p^2)\right\}, \end{aligned}$$

where we have chosen $\hbar = 2$ and used the identity $\hat{a}^\dagger\hat{a} = \frac{1}{4}(\hat{x}^2+\hat{p}^2-2)$. Whilst we are interested in the cases where $g > 1$, there is no such restriction needed for the calculations we will perform here.

To act the Wigner representation of the amplifier on an arbitrary input state requires that the operator product be performed in the Wigner representation. This is achieved by way of the Moyal Product [40] which we will denote $\star$. If we take the input state ρ whose Wigner function is W_ρ then the Wigner function for the output amplified state $\rho' = g^{\hat{a}^\dagger\hat{a}}\rho g^{\hat{a}^\dagger\hat{a}}$ is,

$$W_{\rho'} = G_w \star W_\rho \star G_w \tag{4}$$

We will later show that writing the action of the NLA in this form allows the calculation of compact analytic results for the class of Gaussian states but already the Wigner representation sheds some light upon the unusual properties of this operator.

An interesting point noted in the original proposal [17] is that the NLA will not produce a physical output when acted upon certain input states with certain gains. This does not come as a complete surprise given the state dependent manner in which the transformation is defined, namely over the coherent states. The Wigner representation allows us to understand both the question of physical convergence and Gaussianity of the transformation.

The expression Eq.4 is clearly a Gaussian operation in that it is an exponential quadratic in the phase space variables however for $g > 1$ the expression is a convex, unbounded function in phase space. Nonetheless when the NLA is acted upon a particular input state and the expressions are combined under the appropriate phase space convolution, Eq.4 tells us that if the input state is sufficiently ‘small’ (i.e. in terms of the decay of it’s Wigner function in phase space) relative to the gain of the NLA then the overall output will have a concave, normalisable phase space distribution. That is, the limiting state $\lim_{N\to\inf}\Upsilon_N(\rho)$ is a well defined physical state for this particular situation. Furthermore in this case the NLA will preserve the Gaussianity of the input state in the infinite limit. In section IV we will make rigourous this argument for the restricted class of Gaussian states, give exact criteria for the convergence of the output for a given input.

Finally it is straightforward to see that the operation although mapping Gaussian input to Gaussian outputs, it is not symplectic. This is not in violation of the well known Stone-von Neumann theorem however as the operation also fails to be unitary $g^{\hat{a}^\dagger\hat{a}} = (g^{\hat{a}^\dagger\hat{a}})^\dagger \Rightarrow g^{\hat{a}^\dagger\hat{a}}(g^{\hat{a}^\dagger\hat{a}})^\dagger \neq \mathbb{I}$. We now turn to the problem of evaluating the action of the NLA in this phase space representation upon the Gaussian states. First we will introduce some crucial properties and quantities of these states.

III. SOME PRELIMINARIES OF GAUSSIAN QUANTUM INFORMATION

Within continuous variable quantum information a great deal of attention is devoted to states with a Gaussian Wigner function and operations that preserve this form [41]. These so-called Gaussian states and operations are significant experimentally as they can be efficiently created and implemented and also lend themselves to an elegant theoretical description. This theoretical convenience comes from the fact that although such states live in in infinite dimensional Hilbert space they can be completely characterised by their first and second moments.

In particular if we start N-mode Gaussian state, ρ, living in a tensor product of N infinite dimensional Hilbert spaces equipped with bosonic creation and annihilation operators $\hat{a}_1, \hat{a}_1^\dagger, ...\hat{a}_N, \hat{a}_N^\dagger$ we can use the corresponding quadrature operators $\hat{x}_i = \hat{a}_i + \hat{a}_i^\dagger$ and $\hat{p}_i = i(\hat{a}_i^\dagger - \hat{a}_i)$ as phase space coordinates and completely characterise the state as follows: grouping the quadratures together in a vector $\mathbf{r} := (\hat{x}_1, \hat{p}_1, ..., \hat{x}_N, \hat{p}_N)$ we define any Gaussian state by a displacement (mean) vector,

$$\mathbf{d} = \mathrm{tr}(\rho\mathbf{r}) \tag{5}$$

and covariance matrix

$$\mathbf{\Sigma}_{ij} = \mathrm{tr}\left(\rho\{(\mathbf{r}_i - \mathbf{d}_i), (\mathbf{r}_j - \mathbf{d}_j)\}_+\right) \tag{6}$$

where $\{\}_+$ is the anti-commutator. Matrices will be denoted by boldface throughout and products of such terms should be interpreted as matrix multiplication. For a given square matrix to be a legitimate covariance matrix (CM) it must satisfy the uncertainty principle which in this formalism is the following positive semi-definiteness condition [42],

$$\mathbf{\Sigma} + i\mathbf{\Omega} \geq 0 \tag{7}$$

where

$$\mathbf{\Omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{8}$$

which is called the symplectic form.

The purity of a Gaussian state is obtained simply via the determinant of the CM

$$\mu := \mathrm{tr}(\rho_G^2) = \frac{1}{\sqrt{\det(\mathbf{\Sigma})}} \tag{9}$$

Thus a Gaussian state is pure if and only if we have $\det(\mathbf{\Sigma}) = 1$.

Likewise the entanglement of a Gaussian state is completely determined by the second moments, in particular their symplectic spectra which we obtain by making use of Williamson's theorem [43]. For any N-mode CM $\mathbf{\Sigma}$ there exists a symplectic diagonalisation given by

$$\mathbf{\Sigma} = \mathbf{SWS^T}, \quad \mathbf{W} = \bigoplus_{k=1}^{N} \lambda_k \mathbb{I}, \tag{10}$$

where $\mathbf{S}$ is a symplectic matrix and $\lambda_k \geq 1$ are the N symplectic eigenvalues of $\mathbf{\Sigma}$. They can be computed either by solving an N^{th} order polynomial where the coefficients are so-called symplectic invariants [44] or by finding the standard eigenspectrum of $|i\mathbf{\Omega\Sigma}|$ where the absolute value is used in the operatorial sense [41]. Using the fact that for symplectic matrices $\det(\mathbf{S}) = 1$ the physicality condition for a CM can be rewritten as,

$$\mathbf{\Sigma} > 0, \quad \lambda_- \geq 1 \tag{11}$$

where λ_- is the smallest symplectic eigenvalue

A common bipartite entanglement criteria is to consider the partial transpose (PT) of the density matrix with respect to one subsystem [45, 46], with entanglement (separability) corresponding to the non-physicality (physicality) of the resultant operator. For Gaussian states a similar results hold based upon the CM condition, namely that if we consider the partial transpose of a bipartite $N \times M$ mode CM

$$\tilde{\mathbf{\Sigma}} = (\mathbb{I}_A \oplus \mathbf{T}_B)\mathbf{\Sigma}(\mathbb{I}_A \oplus \mathbf{T}_B) \tag{12}$$

where

$$\mathbf{T}_B := \oplus_{m=1}^{M} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{13}$$

then entanglement corresponds to the non-physicality of $\tilde{\mathbf{\Sigma}}$. It is straightforward to show that we always have $\tilde{\mathbf{\Sigma}} > \mathbf{0}$therefore by Eq.11 the criterion boils down to checking

$$\tilde{\lambda}_- \geq 1. \tag{14}$$

It should be noted that while Eq.14 is generally a necessary condition for bipartite separability it is only necessary and sufficient for $1 \times N$ [47] and the bisymmetric class of $N \times M$ Gaussian states [48]. For such states however one can quantify the entanglement by means of the log negativity [49] which can be computed for continuous variables [50] from the smallest PT symplectic eigenvalue via,

$$\mathcal{E} = \max\{0, \log\tilde{\lambda}_-\} \tag{15}$$

Finally a large class of relevant operations and channels (squeezing, passive mode mixing, amplification and white noise channels) fall in the class of Gaussian operations. These can then be compactly implemented at the level of covariance matrix transformations. In this formalism, Gaussian unitary operations correspond to transformations of the form $\mathbf{\Sigma}_{\mathrm{out}} = \mathbf{S\Sigma}_{\mathrm{in}}\mathbf{S}^T$ where $\mathbf{S}$ is a symplectic matrix. The NLA does not take this symplectic form, nonetheless we will derive analytic input output relations for the amplification of arbitrary Gaussian states.

IV. AMPLIFICATION OF GAUSSIAN STATES

It is inconvenient to evaluate the $\star$ operation in the x and p variables. It is more useful here to write this product down in terms of the characteristic functions (χ) which are the Fourier transform of the corresponding Wigner functions. Here we choose those variables to be a and b corresponding to transformed x and p respectively. With our choice of $\hbar = 2$ (such that the vacuum noise is unity) the product in the Fourier transformed space for operators A and B is:

$$\chi_{AB}(a,b) = \frac{1}{(2\pi)^2}\int da'db'\chi_A(a{-}a', b{-}b')e^{i\mathbf{a}^T\mathbf{\Omega}\mathbf{a}'}\chi_B(a',b') \tag{16}$$

where $\mathbf{a} = (a,b)^T$, $\mathbf{a}' = (a',b')^T$. This formalism carries over to the multidimensional case fairly naturally with the matrix $\mathbf{\Omega}$ extended using the direct sum. The characteristic function for multidimensional Gaussians is

$$\chi_G = e^{i\mathbf{d}^T\mathbf{a}}e^{-\frac{1}{2}\mathbf{a}^T\mathbf{\Sigma}\mathbf{a}} \tag{17}$$

The Moyal product of two Gaussian will then result in another Gaussian. Thus we can simply read off the output covariance matrix and hence overall state from the output characteristic function. Also, we can consider acting amplifiers on all modes and the amplification transformation extends naturally from Eq.4 where we rewrite as

$$G_w(x,p) = \exp\left\{\mathbf{G}^{-1}(x^2+p^2)\right\} \tag{18}$$

we have defined the matrix

$$\mathbf{G} = \begin{pmatrix} \frac{g+1}{g-1} & 0 \\ 0 & \frac{g+1}{g-1} \end{pmatrix} \tag{19}$$

and extend $\mathbf{G}$ to the multimode case by taking the direct sum of all the individual modes. We can take the limit as $g \to 1$ for modes which have no amplification. This limit constitutes a delta function as expected.

To conjugate the density operator by the action of an ideal amplifier the Moyal product must be applied twice. For a Gaussian density operator with mean vector $\mathbf{d}$ and covariance matrix $\mathbf{\Sigma}$ this computation gives two equations for the mean vector and covariance matrix, one from each application of the product.

To compute the relationships for the mean vector and covariance matrix we will utilize the result of the gaussian integral

$$\int dx_1 dx_2 \cdots dx_n e^{-\frac{1}{2}\mathbf{x^T}\cdot\mathbf{A}\cdot\mathbf{x}+\mathbf{b}\cdot\mathbf{x}} \propto e^{\frac{1}{2}\mathbf{b^T}\cdot\mathbf{A^{-1}b}} \tag{20}$$

where this equation holds for matrix $\mathbf{A}$ and vector $\mathbf{b}$ possibly complex (note that the transpose is taken and not the adjoint). We can ignore the proportionality factor here as it can be considered part of the p_N terms we defined in SectionII. Since we are only interested in the convergent state this factor is not relevant.

We will start by computing the left product by the $g^{\hat{a}^\dagger\hat{a}}$ operator $\rho_1 = g^{\hat{a}^\dagger\hat{a}}\rho$ (which is not a physical state) using the Wigner representation and the Moyal product. Substituting in the definitions for the operators results in the integral (ignoring constant proportionality factors)

$$W_{\rho_1} = \int d\mathbf{a}' e^{(\mathbf{a}-\mathbf{a}')^T\mathbf{G}(\mathbf{a}-\mathbf{a}')+i\mathbf{a}'^T\mathbf{\Omega}\mathbf{a}+i\mathbf{d}^T\mathbf{a}'-\frac{1}{2}\mathbf{a}'^T\mathbf{\Sigma}\mathbf{a}'} \tag{21}$$

We can now rearrange the polynomial to obtain an expressions more like that of the standard Gaussian integral.

$$W_{\rho_1} = e^{\frac{1}{2}\mathbf{a}^T\mathbf{G}\mathbf{a}} \int d\mathbf{a}' e^{(i(\mathbf{d}^T+\mathbf{a}^T\mathbf{\Omega})-\mathbf{a}^T\mathbf{G})\mathbf{a}'-\frac{1}{2}\mathbf{a}'^T(\mathbf{\Sigma}-\mathbf{G})\mathbf{a}'} \tag{22}$$

Upon evaluating this integral we find that the covariance matrix transforms as

$$\mathbf{\Sigma}_1 = (i\mathbf{\Omega} - G)(\mathbf{\Sigma} - G)^{-1}(i\mathbf{\Omega} + G) - G \tag{23}$$

and the mean vector transforms as s

$$\mathbf{d}_1 = (i\mathbf{\Omega} - G)(\mathbf{\Sigma} - G)^{-1}\mathbf{d} \tag{24}$$

Following a similar calculation for right multiplying by the amplification operator transforms the covariance matrix as

$$\mathbf{\Sigma}_{out} = (i\mathbf{\Omega} + \mathbf{\Sigma}_1)(\mathbf{\Sigma}_1 - \mathbf{G})^{-1}(i\mathbf{\Omega} + \mathbf{\Sigma}_1) + \mathbf{\Sigma}_1 \tag{25}$$

and the mean vector transforms as

$$\mathbf{d}_{out} = \mathbf{d}_1 - (i\mathbf{\Omega} + \mathbf{\Sigma}_1)(\mathbf{\Sigma}_1 - \mathbf{G})^{-1}\mathbf{d}_1. \tag{26}$$

In the single mode case, $\mathbf{G}$ will be proportional to the identity and hence this can be used to greatly simplify the expressions, but we will work with the case of $\mathbf{G}$ not being proportional to the identity and hence will include multimode cases where different gain variables may be used on different modes.

To simplify these expressions it is important to note that

$$(i\mathbf{\Omega} - \mathbf{G})(i\mathbf{\Omega} + \mathbf{G}) = \mathbb{I} - \mathbf{G}^2. \tag{27}$$

This holds as $\mathbf{G}$ is diagonal and for each local block the two entries are the same. This gives $\mathbf{\Omega}\mathbf{G} = \mathbf{G}\mathbf{\Omega}$ and hence the above relation.

We will now dissect the terms in $\mathbf{\Sigma}_{out}$ and evaluate them:

$$\begin{aligned}(\mathbf{\Sigma}_1 - \mathbf{G})^{-1} \;=\;& (i\mathbf{\Omega} + \mathbf{G})^{-1} \\ & \left[(\mathbf{\Sigma} - \mathbf{G})^{-1} + (i\mathbf{\Omega} + \mathbf{G})^{-1} - (i\mathbf{\Omega} - \mathbf{G})^{-1}\right]^{-1} \\ & (i\mathbf{\Omega} - \mathbf{G})^{-1}\end{aligned} \tag{28}$$

$$\begin{aligned}i\mathbf{\Omega} + \mathbf{\Sigma}_1 \;=\;& (i\mathbf{\Omega} - \mathbf{G})\left[(\mathbf{\Sigma} - \mathbf{G})^{-1} + (i\mathbf{\Omega} + \mathbf{G})^{-1}\right] \\ & (i\mathbf{\Omega} + \mathbf{G})\end{aligned} \tag{29}$$

$$\begin{aligned}i\mathbf{\Omega} - \mathbf{\Sigma}_1 \;=\;& (i\mathbf{\Omega} - \mathbf{G})\left[-(\mathbf{\Sigma} - \mathbf{G})^{-1} + (i\mathbf{\Omega} - \mathbf{G})^{-1}\right] \\ & (i\mathbf{\Omega} + \mathbf{G})\end{aligned} \tag{30}$$

Substituting these results back gives

$$\mathbf{\Sigma}_{out} = \left[(\mathbf{\Sigma} - \mathbf{G})^{-1} - 2(\mathbf{G}^{-1} - \mathbf{G})^{-1}\right]^{-1} - \mathbf{G} \tag{31}$$

This can be further rearranged to give

$$\begin{aligned}\mathbf{\Sigma}_{out} \;=\;& \mathbf{G}^{-1}\left(\mathbf{G}^{-1} + \mathbf{G} - 2\mathbf{\Sigma}\right)^{-1}(\mathbf{\Sigma} - \mathbf{G}) \\ +\;& \mathbf{G}\left(\mathbf{G}^{-1} + \mathbf{G} - 2\mathbf{\Sigma}\right)^{-1}(\mathbf{\Sigma} - \mathbf{G}^{-1})\end{aligned} \tag{32}$$

If instead of using the matrix $\mathbf{G}$ with diagonal elements of the form $\frac{g+1}{g-1}$, we use a matrix

$$\mathbf{g} = \begin{pmatrix} g & 0 \\ 0 & g \end{pmatrix} \tag{33}$$

extended to many modes also using the direct sum, then this matrix equation becomes

$$\begin{aligned}\mathbf{\Sigma}_{out} \;=\;& \mathbf{g}\left[\mathbf{g}^2 + 1 - \mathbf{\Sigma}(\mathbf{g}^2 - 1)\right]^{-1} \\ & \left[\mathbf{\Sigma}(\mathbf{g}^2 + 1) - (\mathbf{g}^2 - 1)\right]\mathbf{g}^{-1}\end{aligned} \tag{34}$$

This equation can be further simplified if we replace the matrix of linear gains $\mathbf{g}$ to a matrix of logarithmic gains

$$\mathbf{l} = \begin{pmatrix} \ln g & 0 \\ 0 & \ln g \end{pmatrix} \tag{35}$$

$$\mathbf{\Sigma}_{out} = (\cosh \mathbf{l} - \mathbf{\Sigma} \sinh \mathbf{l})^{-1} (\mathbf{\Sigma} \cosh \mathbf{l} - \sinh \mathbf{l}). \tag{36}$$

Using the same relationships found above, we can now substitute into the expression for $\mathbf{d}_{out}$ and get

$$\mathbf{d}_{out} = \left[2(\mathbf{\Sigma} - \mathbf{G})(\mathbf{G} - \mathbf{G}^{-1})^{-1} - 1 \right]^{-1} \mathbf{d} \tag{37}$$

and using the $\mathbf{g}$ matrix form gives

$$\mathbf{d}_{out} = 2\mathbf{g} \left[\mathbf{g}^2 + 1 - \mathbf{\Sigma}(\mathbf{g}^2 - 1) \right]^{-1} \mathbf{d} \tag{38}$$

and using the logarithmic gain form gives

$$\mathbf{d}_{out} = (\cosh \mathbf{l} - \mathbf{\Sigma} \sinh \mathbf{l})^{-1} \mathbf{d} \tag{39}$$

We will now use the results from this method to illuminate how we can easily compute the action of the NLA on Gaussian states in one and two-modes.

A. Single-mode states

In general one can unitarily transform one mode Gaussian to remove cross-correlations between the quadratures and hence write CM's of diagonal form,

$$\mathbf{\Sigma} = \begin{pmatrix} V_x & 0 \\ 0 & V_p \end{pmatrix} \tag{40}$$

with relevant examples including thermal, squeezed and coherent states. Considering such states with input mean vector $\mathbf{d} = (\langle \hat{x} \rangle, \langle \hat{p} \rangle)^T$ we transform via 38 to find

$$\mathbf{d}_{NLA} = \begin{pmatrix} \frac{2g\langle x \rangle}{V_x + 1 - g^2(V_x - 1)} \\ \frac{2g\langle p \rangle}{V_p + 1 - g^2(V_p - 1)} \end{pmatrix} \tag{41}$$

Naturally for coherent states ($V_x = V_p = 1$) the above expression reduces to $\mathbf{d}_{\text{out}} = g\mathbf{d}$ but for thermal states ($V_x = V_p = V > 1$) the amplification is no longer linear in g. Instead it increases rapidly and becomes infinite at a maximum value of the gain before becoming negative and as we will see unphysical.

While both thermal and coherent states are phase symmetric, this is not true of squeezed states ($V_x = V^{-1}, V_p = V > 1$) and thus the two quadrature displacements amplify differently. While the anti-squeezed displacement transforms identically to the thermal case the squeezed quadrature displacement amplifies sub-linearly in g. These results are plotted in Fig.1

Turning to the output covariance matrix we can substitute int Eq.34 to obtain,

$$\mathbf{\Sigma}_{NLA} = \begin{pmatrix} \frac{V_x + 1 + g^2(V_x - 1)}{V_x + 1 - g^2(V_x - 1)} & 0 \\ 0 & \frac{V_p + 1 + g^2(V_p - 1)}{V_p + 1 - g^2(V_p - 1)} \end{pmatrix}. \tag{42}$$

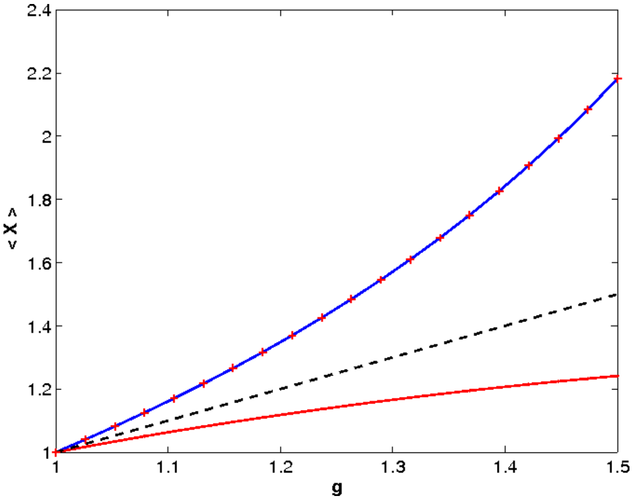

FIG. 1: (colour online) Expectation values of output quadratures $X = \{\hat{x}, \hat{p}\}$ for input coherent (black, dashed), thermal (blue, solid) and squeezed (red, $\hat{x}$ dot-dash, $\hat{p}$ crosses) states. For all plots V = 1.5 and $\mathbf{d} = (1, 1)$.

Following a similar pattern the thermal state variance and that of the anti-squeezed quadrature for the squeezed state become infinite at the same gain for which the squeezed variance vanishes. In other words a thermal state thermalises further whereas a squeezed state is squeezed further Fig.2. Note that this is true regardless of the angle of squeezing. This phase insensitive squeezing property was addressed in [26] where the potential causal paradoxes were resolved.

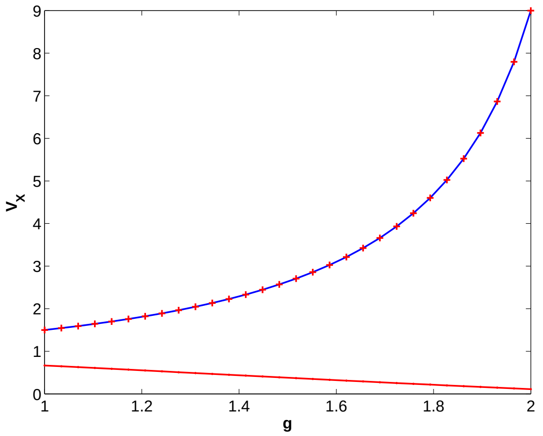

FIG. 2: (colour online) Quadrature variances V_X, $X = \{\hat{x}, \hat{p}\}$ for input thermal (blue, solid) and squeezed (red, $\hat{x}$ dot-dash, $\hat{p}$ crosses) states. For all plots V = 1.5 and $\mathbf{d} = (1, 1)$.

This behaviour is in accord with our intuition from the first section in which we saw evidence for a critical gain at which the output state was described by a flat phase space distribution (infinite variance) and beyond which was unphysical (negative variance).

By considering the output on the single mode case we can derive the necessary and sufficient condition for convergence to a physical output state. Solving for the singularity in the output CM Eq.42 we find that for a single NLA applied to one mode of a multi-mode Gaussian state the maximum physical gain is

$$g_{\max} = \frac{V+1}{V-1}. \tag{43}$$

where V is the variance of the input to the amplifier. Note that in the multi-mode case where more than one NLA is present this condition will be necessary but no longer sufficient to guarantee a convergent output.

B. Two-mode states

The canonical bipartite Gaussian state is the two-mode squeezed vacuum or EPR state which, among other applications, is the building block for quantum teleportation and the theoretical analysis of continuous variable quantum key distribution. In the number basis it has the form,

$$|EPR\rangle = \sqrt{1-\chi^2}\sum_n \chi^n |n\rangle |n\rangle \tag{44}$$

where χ ranges from 0 for an unsqueezed vacuum up to unity for an infinitely squeezed, maximally entangled state.

The effect of the NLA in this context has already been considered in [21] where distillation in the presence of loss was demonstrated and it has also been shown to benefit key distribution over general Gaussian channels [25, 27, 28]. Here we will analytically re-derive the previous results but with much less effort via our new formalism.

An arbitrary Gaussian channel can be described by a transmission T and a thermal noise parameter, for instance the variance of the enivronment V_E.

The covariance matrix of an EPR state with mode B distributed through such a channel is given by,

$$\mathbf{\Sigma}_{\text{in}} = \begin{pmatrix} V_A\ \mathbb{I}_2 & c_{AB}\ \sigma_z \\ c_{AB}\ \sigma_z & V_B\ \mathbb{I}_2 \end{pmatrix} \tag{45}$$

with $\sigma_z = [1,0;0,-1]$ and

$$\begin{aligned} V_A &= \frac{1+\chi^2}{1-\chi^2} \\ V_B &= T\frac{1+\chi^2}{1-\chi^2} + (1-T)V_E \\ c_{AB} &= \frac{2\sqrt{T}\chi}{\chi^2-1} \end{aligned} \tag{46}$$

Again applying Eq.34 where an NLA of gain g is applied to mode B we find an output covariance matrix of the same form as Eq.45 but with entries related to the inputs via

$$\begin{aligned} V_A' &= \frac{1}{N}\ \left[V_A(V_B+1) - T(V_A^2-1)\right. \\ &+ \left. g^2(T(-1+V_A^2) - V_A(-1+V_B))\right] \\ V_B' &= \frac{1}{N}\ \left[V_B + 1 + g^2(V_B-1)\right] \\ c_{AB}' &= \frac{1}{N}\ 2g\sqrt{T(V_A^2-1)} \end{aligned} \tag{47}$$

where

$$N = V_B + 1 - g^2(V_B - 1) \tag{48}$$

which must be positive and non-zero and hence gives the constraint on g outlined in the previous section.

We can now analyse the output states in terms of their entanglement and purity. We know from[17] that for an initially pure EPR state, as the NLA gain reaches it's maximum value the resultant output will tend towards a pure maximally entangled EPR state. The same results were also shown for pure loss channels where, crucially, no entanglement is generated between the transmitted mode and the environment. As soon as there is decoherence any amount of decoherence the NLA wtill start to distill correlations between the amplified mode and the noisy environment as well as the other arm of the EPR. Thus it becomes impossible to distill maximal entanglement within the allowable gain range. We will consider the entanglement distillation in the presence of Gaussian decoherence via the logarithmic negativity given in Eq.15. For two-mode states with CM of the form Eq.45 the symplectic eigenvalues of the PT state are given by,

$$\tilde{\lambda}_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det(\tilde{\mathbf{\Sigma}})}}{2}} \tag{49}$$

where $\Delta := a^2 + b^2 + 2c^2$ and $\det(\tilde{\mathbf{\Sigma}}) = \det(\mathbf{\Sigma}) = (ab - c^2)^2$. In Fig.3 we plot the logarithmic negativity as a function of gain for the ideal channel and for increasing levels of decoherence.

We paramaterise the channel by fixing the initial variance (V_A) (or alternatively the EPR paramater χ) of the EPR to be distributed and the variance of a thermal environment mode V_E and then interacting the two modes on a beamsplitter of varying transmission. A perfect channel corresponds to $T = 1$ with an increasingly mixed output for smaller values. For the cases plotted we have $V_E < V_A$ so as the transmission decreases so does Bob's variance leading to a higher maximum allowable gain. These results show the entanglement increasing monotonically as a function of g. While a perfect channel allows for maximum distillation, modest amounts of loss and noise swiftly decrease the maximum distillable entanglement and the rate of increase with g.

We are also interested in the purity of our final state, and by considering Eq.9 it is swiftly apparent that the

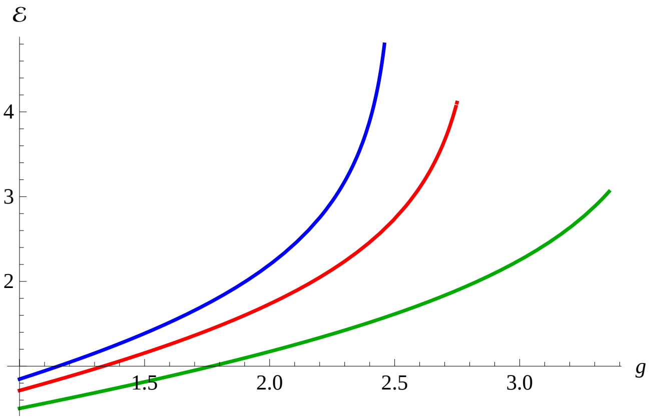

FIG. 3: (colour online) Logarithmic negativity of an amplified EPR state as a function of gain for varying levels of channel decoherence. We paramaterise this by fixing an initial EPR strength of $\chi = 0.4$ ($V_A \approx 1.4$) and a thermal environment of variance $V_E = 1.1$ and mixing the two on beamsplitter of decreasing transmission T. Plotted curves are for $T = 1$ (blue), $T = 0.8$ (red) and $T = 0.5$.

purity decreases monotonically with gain and that

$$\lim_{g \to gmax} \mu = 0. \tag{50}$$

We plot the purity of the output states corresponding to those shown in Fig.3 demonstrating the degradation of purity as a function of gain. We see that the decay is initially gentle and then rapidly decreases as the maximum gain is approached. Thus we are left with a further restriction upon the maximum distillable entanglement if we would also like to maintain high levels of purity.

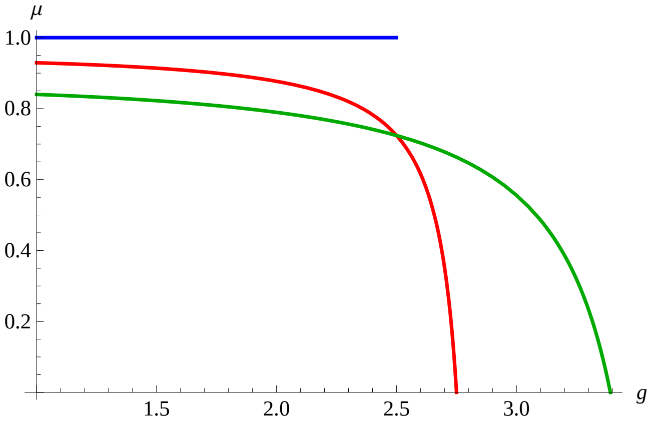

FIG. 4: (colour online) Purity of an amplified EPR state as a function of gain for the same input parameters as Fig.3. Once again Plotted curves are for $T = 1$ (blue), $T = 0.8$ (red) and $T = 0.5$

These results demonstrate the competing considerations of entanglement strength and purity that must be taken into account when choosing the NLA gain to be applied. In the previous discussion ignored the final degree of freedom available to Alice and Bob, namely the strength of the input EPR. For example in a situation where the purity of entanglement is of great importance Alice and Bob can attempt to improve their protocol by starting with weaker entanglement and amplifying it further after the channel. As a further example of the utility of our formalism is the ease with which one can optimise over input parameters to maximise a desired operational quantity. As a demonstration we will plot the maximum achievable fidelity between the de-cohered and subsequently amplified EPR state and a pure target EPR state of a certain strength. We plot the results as a function of the target EPR parameter χ_T where both input EPR strength and the NLA gain have been optimised over. The fidelity between two-mode Gaussian states of zero mean is given by [51],

$$F = \frac{1}{\sqrt{\Gamma} + \sqrt{\Lambda} - \sqrt{(\sqrt{\Gamma} + \sqrt{\Lambda})^2 - \Theta}} \tag{51}$$

where

$$\begin{aligned}
\Gamma &= \frac{1}{16}\left[1 - 2c_{AB}c'_{AB} + V_A\left(-V_B\left(c'_{AB}\right)^2 + V'_A\right)\right. \\
&+ \left. V_B\left(1 + V_A V'_A\right)V'_B + c_{AB}^2\left(\left(c'_{AB}\right)^2 - V'_A V'_B\right)\right]^2 \\
\Lambda &= \frac{1}{16}\left(c_{AB}^4 + c_{AB}^2\left(2 - 2V_A V_B\right) + \left(-1 + V_A^2\right)\left(-1 + V_B^2\right)\right) \\
&\times \left[\left(c'_{AB}\right)^4 + \left(c'_{AB}\right)^2\left(2 - 2V'_A V'_B\right) + \left(-1 + \left(V'_A\right)^2\right)\right. \\
&\left.\left(-1 + \left(V'_B\right)^2\right)\right] \\
\Theta &= \frac{1}{16}\left(\left(c_{AB} + c'_{AB}\right)^2 - \left(V_A + V'_A\right)\left(V_B + V'_B\right)\right)^2
\end{aligned} \tag{52}$$

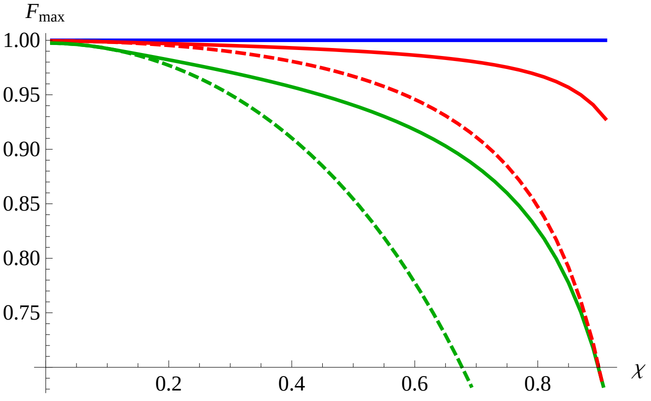

FIG. 5: (colour online) Maximum fidelity between a distributed EPR state after amplification and a pure target EPR state as a function of the target EPR strength χ_T for varying levels of channel decoherence. We paramaterise the channel by fixing a thermal environment of variance $V_E = 1.01$ and mixing the two on beamsplitter of decreasing transmission T. Plotted curves are for $T = 1$ (blue), $T = 0.9$ (green) and $T = 0.5$ red). For all points the NLA gain and input EPR strength are simultaneously optimised over. To illustrate the improvement due to amplfication we also plot the performance in the absence of an NLA (dashed lines) for comparison.

where the input covariance matrices are in standard form with entries V_A, V_B, c_{AB} and V_A', V_B', c_{AB}' respectively. This expression differs slightly from that given in [51] as we have a different noise convention with our vacuum normalised to 1 instead $\frac{1}{2}$.

V. EFFECTIVE CIRCUIT

In the previous section we derived the effect of the NLA upon an EPR state transmitted through an arbitrary Gaussian channel and calculated the strength and purity of the resultant entanglement. The same situation was also considered in [25, 27, 28] for the purposes of Continuous Variable Quantum Key Distribution (CVQKD) where the authors paramaterised the results in terms of an effective combination of a different EPR state and channel. However if we pursue this representation in detail we find that although such a description is helpful as a tool for conceptualising how the NLA will affect communication rates it is insufficient to describe the true nature of correlations with an eavesdropper (Eve).

One can attempt to solve for a set of effective parameters T', ξ', χ', where the ξ is another noise parameter more commonly used the CVQKD literature. It is defined by setting the total variance added by the channel environment to be $V_E = \frac{1-T+T\xi}{1-T}$. From this formula it is apparent that the added channel noise has been split up into a component due to loss and the so-called excess noise ξ. In these papers the output of the NLA corresponds to a scenario where Alice created a stronger EPR initially and transmitted it through an effective channel. Setting the equations in Eqs.46 and 47 equal we obtain,

$$\begin{aligned} \chi' &= \sqrt{1+\frac{2T(1-g^2))}{g^2T\xi-T\xi-2)}}\chi \\ T' &= \frac{4g^2T}{(-2+(-1+g^2)T(-2+\xi))(-2+(-1+g^2)T\xi)} \\ \xi' &= -\frac{1}{2}(-2+(-1+g^2)T(-2+\xi))\xi. \end{aligned} \tag{53}$$

The secret key rates of the previous works are of course correct as they only depend upon the reduced covariance matrix shared by Alice and Bob, however this interpretation is not always valid and it turns out does not fully capture the correlations generated by the NLA.

In general one assumes that all of the observed noise originates from the eavesdropper interactions, in other words that Eve purifies the state. For a noisy Gaussian channel where Bob's mode is effectively mixed with a thermal state a valid purification is for Eve to have her own EPR state and interact one arm with Bob's mode.

Consider the symmetrical case where Alice and Eve create identical EPR pairs and interact them upon a 50:50 beamsplitter. If Bob applies an NLA and we ask about his correlations with Alice and then Eve then the previous analysis results in a contradiction. If we consider the Alice-Bob channel we we see the effective transmission increase, but if we consider the Eve-Bob channel exactly the same result should hold. Clearly the beamsplitter ratio cannot simultaneously increase and decrease and we arrive at a contradiction.

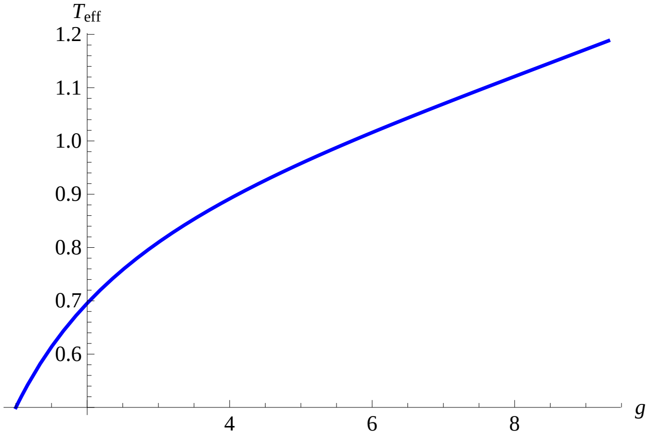

FIG. 6: Effective channel transmission as a function of gain, as given by Eq.53. Input parameters are the same as Fig.3 with $T = 0.5$. The curve is only plotted for gains less than the maximum allowed value but the effective transmission still exceeds the maximum sensible value for a beamsplitter.

In fact if we plot the effective transmission given in Eq.53 as a function of gain, Fig.6, we see that for large but allowable gains they cease to make physical sense. In particular the effective channel transmission can surpass unity, indicating that the NLA can not always effectively be equated with a beamsplitter interaction. Note that although this effective paramaterisation has broken down, key rates calculated by considering only the reduced covariance matrix are still valid as the entropies are independent of Eve's particular purification. Nonetheless we are interested in ascertaining the exact form of the interaction given by the NLA.

The ease with which our method can be adapted to a multi-mode picture allows us to straightforwardly answer this question by explicitly including Eve's modes in the calculation and explicitly analysing the correlations. We consider the situation where Eve makes an entangling cloner attack as per the upper panel of Fig.7, mixing one arm of her own EPR with Bob's mode on a beamsplitter of transmission T. Bob subsequently applies an NLA before detection. The initial 4-mode covariance matrix looks like,

$$\mathbf{\Sigma} = \begin{pmatrix} V\ \mathbb{I}_2 & c_{AB}\ \sigma_z & 0 & 0 \\ c_{AB}\ \sigma_z & V\ \mathbb{I}_2 & 0 & 0 \\ 0 & 0 & V_E\ \mathbb{I}_2 & c_{E1E2}\ \sigma_z \\ 0 & 0 & c_{E1E2}\ \sigma_z & V_E\ \mathbb{I}_2 \end{pmatrix} \tag{54}$$

with $c_{AB} = \sqrt{V^2-1}$ and $c_{E1E2} = \sqrt{V_E^2-1}$. The final CM is obtained by enacting a beamsplitter transformation between Bob's mode (B) and the first eavesdropping mode (E1) that is, $\mathbf{\Sigma} \to \mathbf{BS}_{BE1}(T)\mathbf{\Sigma}\mathbf{BS}_{BE1}^T(T)$ and then substituting this into Eq.34. This results in,

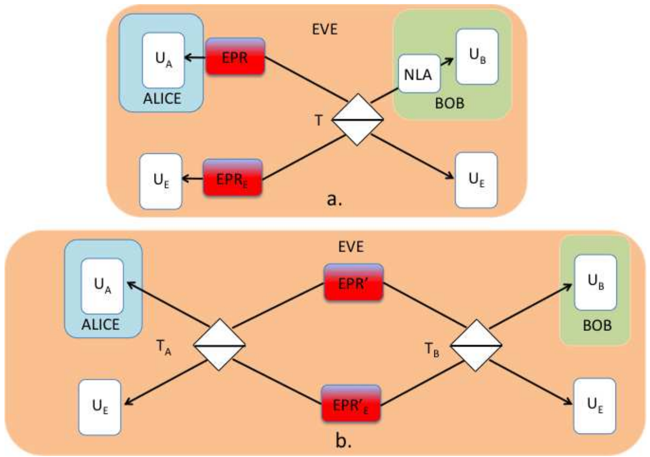

FIG. 7: Equivalent eavesdropper attack in the presence on an NLA: a) In the original scenario Alice and Eve each create EPR which they mix on a beamsplitter of transmission T with the transmitted mode being sent to Bob, who uses an NLA. b) The correlations generated by this are identical to an equivalent scenario where Eve mixes her unused EPR arm with Alice's mode on a beamsplitter of transmission T_A while the original beamsplitter changes transmission to a different value T_B. Both effective EPR pairs also increase in entanglement.

$$\mathbf{\Sigma}_{NLA} = \begin{pmatrix} V_A\ \mathbb{I}_2 & c_{AB}\ \sigma_z & c_{AE1}\ \sigma_z & c_{AE2}\ \mathbb{I}_2 \\ c_{AB}\ \sigma_z & V_B\ \mathbb{I}_2 & c_{BE1}\ \mathbb{I}_2 & c_{BE2}\ \sigma_z \\ c_{AE1}\ \sigma_z & c_{BE1}\ \mathbb{I}_2 & V_{E1}\ \mathbb{I}_2 & c_{E1E2}\ \sigma_z \\ c_{AE2}\ \mathbb{I}_2 & c_{BE2}\ \sigma_z & c_{E1E2}\ \sigma_z & V_{E2}\ \mathbb{I}_2 \end{pmatrix} \tag{55}$$

where,

$$\begin{aligned} V_A &= V + T + (1-T)VV_E \\ &+ g^2(V - T - (1-T)VV_E) \\ V_B &= TV + (1-T)V_E + 1 \\ &+ g^2(TV + (1-T)V_E) - 1) \\ V_{E1} &= (1-T)V + TV_E + VV_E \\ &+ g^2((1-T)V + TV_E - VV_E) \\ V_{E2} &= V_E + 1 + T(VV_E - 1) \\ &+ g^2(V_E - 1 - T(VV_E - 1)) \\ c_{AB} &= 2g\sqrt{T(V^2-1)} \\ c_{AE1} &= -(V_E+1)\sqrt{(1-T((V^2-1)} \\ &+ g^2(V_E - 1 - T(VV_E - 1)) \\ c_{BE1} &= 2g\sqrt{(1-T)T}(V - V_E) \\ c_{BE2} &= 2g\sqrt{(1-T)(V_E^2-1)} \\ c_{E1E2} &= 2g\sqrt{(1-T)(V_E^2-1)} \\ c_{AE2} &= (g^2-1)\sqrt{(1-T)T(V^2-1)(V_E^2-1)} \end{aligned} \tag{56}$$

The elements of the reduced CM shared between Alice and Bob are exactly the same as in the previous section, however if we consider the correlations with the eavesdropper we notice an extremely unusual feature. Ordinarily for any Gaussian channel acting solely upon Bob's side the correlation between Alice's mode and the eavesdroppers non-interacted mode, c_{AE2}, is identically zero. However examining this term in Eq.56 we find that whenever $g \neq 1$ there are correlations despite the fact these modes never interacted.

Such correlations could never be reproduced by an effective setup of the form of the top panel of Fig.7 so we are motivated to construct an equivalent setup including an eavesdropping attack on both Alice's and Bob's modes as per the bottom panel of Fig.7. This would produce a CM given by,

$$\begin{aligned} \mathbf{\Sigma}_{\text{equiv}} &= \mathbf{BS}_{AE2}(T_A)\mathbf{BS}_{BE1}(T_B)\mathbf{\Sigma} \\ &\quad \mathbf{BS}^T_{BE1}(T_B)\mathbf{BS}^T_{AE2}(T_A) \end{aligned} \tag{57}$$

If we equate Eq.56 and Eq.57 some lengthy algebra does result in a unique solution for the effective scenario where Eve interacts one EPR mode with Alice and one with Bob. The expressions for these effective parameters are given in detail in Appendix A.

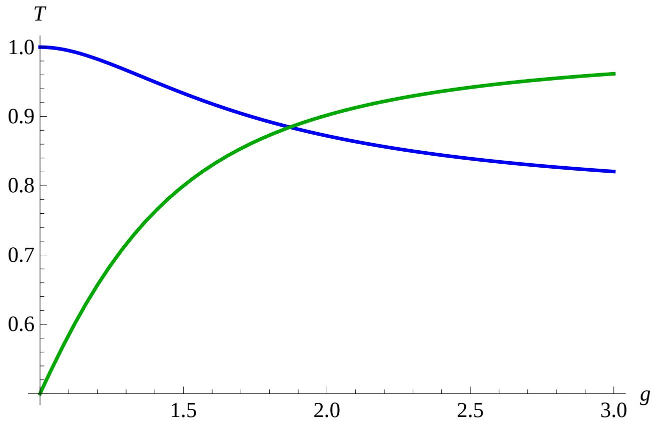

FIG. 8: Effective channel transmission Alice's (T_A) and Bob's (T_B) side as a function of the NLA gain. The input parameters are $T = 0.5$ and $V_E = 1.1$. As the NLA gain increases the channel on Alice's side worsens (T_A decreases) whereas the channel on Bob's side improves (T_B increases) asymptoting to a perfect channel on Bob's side with the attack now exclusively on Alice's side.

Considering the same initial state and channel as the previous section the effective channel parameters reveal an intriguing conclusion about the effect of the NLA. As the NLA gain increases the channel on Bob's side improves (i.e. the effective transmission increases) whereas the converse is true of Alice's side as shown in Fig.8. In fact for these parameters the attack on Bob's side disappears almost entirely.

Finally we also see that both Alice and Eve's effective initial entanglement is increased though not equitably. The variance characterising Eve's effective EPR increases modestly as the gain approaches it's maximum whereas

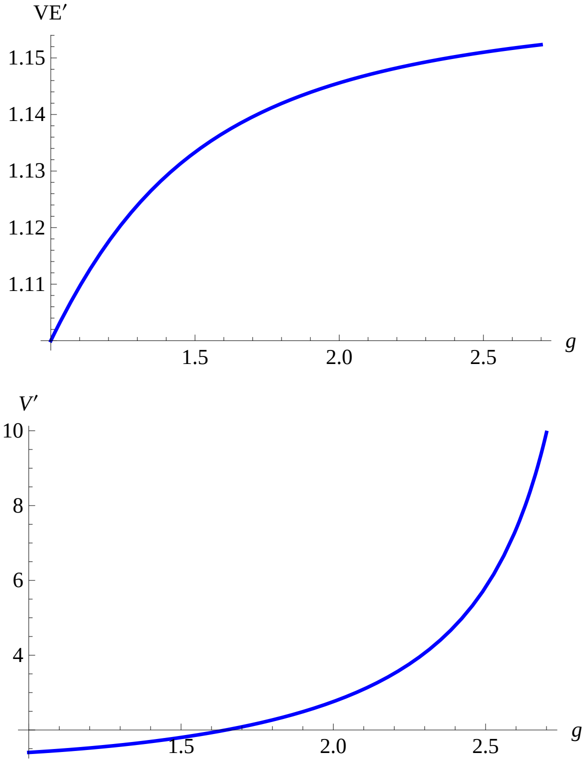

FIG. 9: Effective entanglement for Alice (bottom panel) and Eve (top panel) paramaterised by their variance as a function of the NLA gain. The input parameters are $T = 0.5$ and $V_E = 1.1$. The effective entanglement of both parties increases as a function of the gain.

Alice's diverges as expected from the previous thermal state results.

VI. CONCLUSIONS

In conclusion we have considered the phase space representation of an ideal NLA, gaining insight into the regimes resulting in physical outputs for input states other than coherent states, explaining this in terms of the relative divergence of the NLA and the target state in phase space. For Gaussian states we have derived compact analytic formula's for the action of up to N amplifiers upon N-mode states. We have given explicit results for important examples in one and two modes and analysed the strength and purity of entanglement of EPR states through general Gaussian decoherence, demonstrating that our methods allow for the swift identification of the best strategy for a given protocol. Finally we uncovered some intriguing effects on correlations between two, two-mode entangled states with the counterintuitive result that under amplification an interaction is moved from one side to another.

Future work of great practical importance will be to investigate various proposals for implementations of the NLA, especially the promising post-selection approaches of [27, 28], to determine corresponding success probabilities which are critical for protocols where the rate is of great importance such as QKD and metrology. Finally other results enabled by this work will include revisiting various canonical quantum information tasks such as cloning and state discrimination.

Acknowledgements.— The authors would like to thank S. Rahimi-Keshari for useful discussions. This research was conducted by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project number CE11000102)

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[2] S. Braunstein and H. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[3] C. H. Bennett and G. Brassard (Proceedings of International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984).

[4] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[5] C. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[6] S. Braunstein and H. Kimble, Phys. Rev. A **61**, 042302 (2000).

[7] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature **390**, 575 (1997).

[8] A. Furusawa, J. Sørensen, S. Braunstein, C. Fuchs, H. Kimble, and E. Polzik, Science **282**, 706 (1998).

[9] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptology **5**, 3 (1992).

[10] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[11] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[12] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Opt. Express, OE **19**, 10387 (5).

[13] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati,

J. F. Dynes, et al., New Journal of Physics **11**, 075001 (2009).

[14] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, et al., Nature (2012).

[15] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, et al., Nature **488**, 185 (2012).

[16] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).

[17] T. C. Ralph and A. P. Lund, *Quantum Communication Measurement and Computing Proceedings of 9th International Conference* p. 155 (2009).

[18] P. Marek and R. Filip, Physical Review A **81**, 022302 (2010).

[19] J. Fiurášek, Physical Review A **80**, 053822 (2009).

[20] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 70501 (2010).

[21] T. C. Ralph, Physical Review A **84**, 022339 (2011).

[22] S.-Y. Lee, S.-W. Ji, H.-J. Kim, and H. Nha, Physical Review A **84**, 012302 (2011).

[23] D. Pitkanen, X. Ma, R. Wickert, P. V. Loock, and N. Lütkenhaus, Physical Review A **84**, 022325 (2011).

[24] J. Brask, N. Brunner, D. Cavalcanti, and A. Leverrier, Phys. Rev. A **85**, 042116 (2012).

[25] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[26] C. Gagatsos, E. Karpov, and N. J. Cerf, Phys. Rev. A **86**, 012324 (2012).

[27] J. Fiurasek and N. J. Cerf, arXiv (2012), 1205.6933v1.

[28] N. Walk, T. Symul, P. K. Lam, and T. C. Ralph, arXiv (2012), 1206.0936v2.

[29] F. Ferreyrol, N. Spagnolo, R. Blandino, M. Barbieri, and R. Tualle-Brouri, arXiv (2012), 1205.6195v1.

[30] H.-J. Kim, S.-Y. Lee, S.-W. Ji, and H. Nha, Physical Review A **85**, 013839 (2012).

[31] C. Navarrete-Benlloch, R. García-Patrón, J. Shapiro, and N. Cerf, Phys. Rev. A **86**, 012328 (2012).

[32] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nature Photonics **4**, 316 (2010).

[33] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).

[34] A. Zavatta, J. Fiurášek, and M. Bellini, Nature Photon **5**, 52 (2011).

[35] M. A. Usuga, C. R. Müller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nat Phys **6**, 767 (2010).

[36] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, Phys. Rev. A **83**, 063801 (2011).

[37] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde, arXiv (2012), 1208.5881v1.

[38] M. Micuda, I. Straka, M. Mikova, M. Dusek, N. J. Cerf, J. Fiurasek, and M. Jezek, arXiv (2012), 1206.2852v1.

[39] C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R. T. Thew, arXiv (2012), 1203.3396v2.

[40] J. Moyal, Mathematical Proceedings of the Cambridge Philosophical Society **45**, 99 (1949).

[41] C. Weedbrook, S. Pirandola, R. García-Patrón, N. Cerf, T. Ralph, J. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[42] R. Simon, N. Mukunda, and B. Dutta, Phys. Rev. A **49**, 1567 (1994).

[43] J. Williamson, American journal of mathematics **58**, 141 (1936).

[44] A. Serafini, Phys. Rev. Lett. **96**, 110402 (2006).

[45] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[46] M. Horodecki, P. Horodecki, and R. Horodecki, Physics Letters A **223**, 1 (1996).

[47] R. Werner and M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).

[48] G. Adesso and F. Illuminati, J. Phys. A: Math. Theor. **40**, 7821 (2007).

[49] G. Vidal and R. Werner, Physical Review A **65**, 032314 (2002).

[50] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).

[51] P. Marian and T. Marian, Phys. Rev. A **86**, 022340 (2012).

Appendix A: 4-mode equivalent circuit

Here we derive in detail the parameters for the effective circuit shown in the bottom panel of Fig.7. We start with two EPR pairs belonging to Eve and Alice, parameterised by variances V', V'_E respectively. To calculate the necessary output CM's we need the NLA transform given by Eq.34 and the 4-mode version of the beamsplitter transform. This induces correlations between the two target modes and acts as the identity upon the others. For example the 4-mode beamsplitter matrix acting upon modes 2 and 3 with transmission T is,

$$\mathbf{BS}_{2,3}(T) = \begin{pmatrix} \mathbb{I}_2 & 0 & 0 & 0 \\ 0 & \sqrt{T}\ \mathbb{I}_2 & -\sqrt{1-T} & 0 \\ 0 & \sqrt{1-T}\ \sigma_z & \sqrt{T}\ \mathbb{I}_2 & 0 \\ 0 & 0 & 0 & \mathbb{I}_2 \end{pmatrix} \tag{A1}$$

Note that the minus sign that appears on one of the correlation terms is essentially a choice of convention, or corresponds to a choice to swap which mode enters which port of the beamsplitter.

In this purified version of the protocol the transmission through the channel simply corresponds to mixing modes B (2) and and E1(3) via A1

$$\mathbf{\Sigma}_{\text{ch}} = \mathbf{BS}_{B,E1}(T)\mathbf{\Sigma}\mathbf{BS}^T_{B,E1}(T) \tag{A2}$$

and the substituting this into Eq.34 which directly gives the terms in Eq.56. We now calculate the equivalent circuit CM given by Eq.57 which has the block diagonal form of Eq.45 with

$$V_A \ = \ V'_E + T_A(V' - V'_E)$$

$$\begin{aligned}
V_B &= V_E' + T_B(V' - V_E') \\
V_{E1} &= T_B(V_E' - V') + V' \\
V_{E2} &= T_A(V_E' - V') + V' \\
c_{AB} &= -\sqrt{(1-T_A)(1-T_B)(V_E'^2 - 1)} + \sqrt{T_A T_B (V'^2 - 1)} \\
c_{AE1} &= -\sqrt{(1-T_A)T_B(V_E'^2 - 1)} - \sqrt{T_A(1-T_B)(V'^2 - 1)} \\
c_{BE1} &= \sqrt{(1-T_B)T_B}(V_E' - V') \\
c_{BE2} &= \sqrt{T_A(1-T_B)(V_E'^2 - 1)} + \sqrt{(-1+T_A)T_B(1-V'^2)} \\
c_{E1E2} &= \sqrt{T_A T_B (V_E'^2 - 1)} - \sqrt{(1-T_A)(1-T_B)(V'^2 - 1)} \\
c_{AE2} &= \sqrt{(1-T_A)T_A}(V' - V_E')
\end{aligned} \tag{A3}$$

We now wish to set this expression equal to Eq.56 simultaneously solve for V', V_E', T_A, T_B. In practice one an proceed by considering only a few terms and then checking that the solution satisfies all terms. By equating the variance terms one can swiftly solve for three of the parameters in terms of the fourth and the input variables obtaining,

$$\begin{pmatrix} T_A \\ \\ T_B \\ \\ V_E' \end{pmatrix} = \begin{pmatrix} \frac{(1+V_E)(-1+V')+T(1-VV_E+VV'-V_EV')+g^2((1-V_E)(1+V')+T(-1+VV_E-VV'+V_EV'))}{(-1-V)(1+V_E)+2(1+T(V-V_E)+V_E)V'+g^2((-1+V)(-1+V_E)-2(-1+T(V-V_E)+V_E)V')} \\ \\ \frac{\left(-1-g^2\right)TV_E+\left(1+g^2+\left(-1+g^2\right)(-1+T)V_E\right)V'+V\left(-1+T-V_E+TV'+g^2(-1+T+V_E-TV')\right)}{(-1-V)(1+V_E)+2(1+T(V-V_E)+V_E)V'+g^2((-1+V)(-1+V_E)-2(-1+T(V-V_E)+V_E)V')} \\ \\ \frac{(-1-V)(1+V_E)+(1+T(V-V_E)+V_E)V'+g^2(1+V'+V_E(-1+(-1+T)V')+V(-1+V_E-TV'))}{-1-TV+(-1+T)V_E+g^2(-1+T(V-V_E)+V_E)} \end{pmatrix} \tag{A4}$$

Considering, say, the c_{AE2} correlation term we find a quadratic with the two solutions corresponding to a permutation of the roles of Alice and Eve. Considering any of the other correlation terms will yield only one consistent solution. One further subtlety is apparent upon considering the c_{AE2} term. In particular the expression Eq.56 is always positive whereas the corresponding term in Eq.A3 changes sign depending upon the relative magnitude of V and V_E. The resolution to this is that for situations where the original parameters are such that $V_E > V$ we must change the phase convention for the beamsplitter on Alice's side. This corresponds to moving the minus sign in Eq.A1 to the other correlation term. The two solutions for the remaining parameter V' are,

$$V' = \begin{cases} \frac{g^2(-1+V)(-1+V_E)-(1+V)(1+V_E)-\sqrt{B^2+4C}}{2(-1-TV+(-1+T)V_E+g^2(-1+T(V-V_E)+V_E))}, & V > V_E \\ \\ \frac{g^2(-1+V)(-1+V_E)-(1+V)(1+V_E)+\sqrt{B^2+4C}}{2(-1-TV+(-1+T)V_E+g^2(-1+T(V-V_E)+V_E))}, & V < V_E \end{cases} \tag{A5}$$

where

$$\begin{aligned}
B &= 1 + V + V_E + VV_E + g^2(-1 + V + V_E - VV_E) \\
C &= \left(-1 - TV + (-1+T)V_E + g^2(-1 + T(V - V_E) + V_E)\right)\left(\left(1 - g^2\right)TV_E + V\left(1 - T + V_E + g^2(-1 + T + V_E)\right)\right)
\end{aligned}$$

Direct substitution then confirms that for all input parameters we have a unique set of parameters that yield an identical CM to that created by the NLA.